Solutions to the homework

Joep Horbach

November 18th 2013

Exercise 1

Let $n > 1$, let $u, x, z \in \mathbb{Z}$ and suppose the following conditions hold:

$$nz + nx - 1|^n n^2u - (nx-1)^2$$

$$2nz + 1|^n nx - 1$$

$$2nz - 1|^n nx - 1$$

$$2n^2u + 1|^n nx - 1$$

We want to prove that $u = z^2$.

a) Using the first condition, prove that $nz + nx - 1|n^2u - n^2z^2$.

Solution: If $x|^n y$ then there exist q and f such that $yn^f = xq$. If x and n are relatively prime, this gives us that $n^f|q$ must hold. Define $k := \frac{q}{n^f} \in \mathbb{Z}$, then $y = xk$ and so $x|y$. Because $nz + nx - 1$ is obviously relatively prime to n, we get $nz + nx - 1|n^2u - (nx-1)^2$. We also know $nz + nx - 1|(nz + nx - 1)(nz - (nx - 1))$, so $nz + nx - 1|n^2z^2 - (nx-1)^2$, so $nz + nx - 1|n^2u - (nx-1)^2 - (n^2z^2 - (nx-1)^2)$ and so $nz + nx - 1|n^2u - n^2z^2$.

Assume $u \neq z^2$

b) Prove that $|nx - 1| - n|z| \leq n^2|u| + n^2z^2$.

Solution: Since $n > 1$ and $u \neq z^2$, we know $n^2u - n^2z^2 \neq 0$. Because $nz + nx - 1|n^2u - n^2z^2$ it now follows that $|nz + nx - 1| \leq |n^2u - n^2z^2|$. So we get $|nx - 1| - n|z| = |nx - 1| - |-nz| \leq |nz + nx - 1| \leq |n^2u - n^2z^2| \leq |n^2u| + |n^2z^2| = n^2|u| + n^2z^2$.

c) Using the second and third condition, prove that $(2nz + 1)(2nz - 1)|nx - 1$ and therefore that $4n^2z^2 - 1 \leq |nx - 1|$.

Solution: Again because $2nz + 1$ and $2nz - 1$ are both relatively prime to n, it follows from the second and third condition that $2nz + 1|nx - 1$ and $2nz - 1|nx - 1$. $2nz + 1$ and

$2nz-1$ are both odd and differ only by 2 so must be relatively prime to each other. Both divide $nx-1$ so we get $(2nz+1)(2nz-1)|nx-1$. $n>1$ and $x\in\mathbb{Z}$ so $nx-1\neq 0$. Therefore we get $|(2nz+1)(2nz-1)|\leq|nx-1|$ and so $4n^2z^2-1\leq|4n^2z^2-1|\leq|nx-1|$.

d) Using the fourth condition, prove that $2n^2|u|-1\leq|nx-1|$ and combining this with b) and c), show that $(n|z|)^2-n|z|-1\leq 0$.

Solution: $2n^2u+1$ is relatively prime to n, so from the fourth condition it follows that $2n^2u+1|nx-1$. Like before, $nx-1\neq 0$, so $|2n^2u+1|\leq|nx-1|$ and so $2n^2|u|-1=|2n^2u|-|-1|\leq|2n^2u+1|\leq|nx-1|$. Because $4n^2z^2-1\leq|nx-1|$ and $2n^2|u|-1\leq|nx-1|$, we also have $\frac{1}{2}(4n^2z^2-1+2n^2|u|-1)=2n^2z^2+n^2|u|-1\leq|nx-1|$. We have $|nx-1|-n|z|\leq n^2|u|+n^2z^2$, so combining these two gives us $2n^2z^2+n^2|u|-1-n|z|\leq n^2|u|+n^2z^2$ which is easily reduced to $(n|z|)^2-n|z|-1\leq 0$.

e) Conclude that $u=z^2$ must hold.

Solution: Assume $z=0$, then from $|nx-1|-n|z|\leq n^2|u|+n^2z^2$ it follows that $|nx-1|\leq n^2|u|$. We also have $2n^2|u|-1\leq|nx-1|$, so we get $2n^2|u|-1\leq n^2|u|$, so $n^2|u|\leq 1$, but because $n>1$, we must have $u=0$, which contradicts $u\neq z^2$. Assume $z\neq 0$, then $n|z|$ is at least 2, because $n>1$, but then $(n|z|)^2-n|z|-1\leq 0$ can not possibly hold. We conclude that our assumption that $u\neq z^2$ was wrong and that $u=z^2$ must hold.

Exercise 2

Prove that for any integer $d\neq 0$, there exists an integer x such that $x|^n1$ and $d|^n nx-1$. Hint: Split d into two parts and consider the Euler-Phi function on one of these parts.

Solution: Write $d=ab$ where a only contains prime factors that are also in n while b is relatively prime to n. Define $x=n^{\phi(b)-1}$. Now $x|^n1$ because x is a power of n so the first part holds. Because a only contains prime factors that are also in n, a will divide some power of n and so we can find $f,q\in\mathbb{Z}$ such that $qa=n^f$. Also note that $n^{\phi(b)}\equiv 1 \mod b$ because b and n are relatively prime, so $nx-1=n^{\phi(b)}-1\equiv 0 \mod b$ and so we can write $nx-1=kb$ for some $k\in\mathbb{Z}$. Combining these things gives us $(qk)d=(nx-1)n^f$ and so $d|^n nx-1$.

Grading

Exercise 1

a) $\frac{1}{2}$ points for showing $nz+nx-1|n^2u-(nx-1)^2$. $\frac{1}{2}$ points for finishing the proof.

b) $\frac{1}{2}$ points for showing $|nz+nx-1|\leq|n^2u-n^2z|$. $\frac{1}{2}$ points for finishing the proof.

c) $\frac{1}{2}$ points for showing $2nz + 1|nx - 1$ and $2nz - 1|nx - 1$. $\frac{1}{2}$ points for showing $(2nz + 1)(2nz - 1)|nx - 1$. $\frac{1}{2}$ points for showing $4n^2z^2 - 1 \leq |nx - 1|$

d) $\frac{3}{4}$ points for showing $2n^2|u| - 1 \leq |nx - 1|$ and $\frac{5}{4}$ points for showing $(n|z|)^2 - n|z| - 1 \leq 0$.

e) 1 point for correctly finding a contradiction when $z = 0$. 1 point for correctly finding a contradiction when $z \neq 0$.

Exercise 2

$\frac{1}{2}$ points for correctly splitting d into two components. 1 point for correctly defining x. $\frac{1}{2}$ points for showing $x|^n 1$ holds for this x. $\frac{1}{2}$ points for showing $d|^n nx - 1$ holds.

Note: If the same mistake is made twice, it will only be counted as wrong the first time.